TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. CHA920010001US1

In Re Application Of: **Tresser**

Application No. 09/779,954	Filing Date 02/09/2001	Examiner Elisca, P.	Customer No. 23550	Group Art Unit 3621	Confirmation No. 7575

Invention: **SYSTEM AND METHOD FOR MAINTAINING CUSTOMER PRIVACY**

OIPE JC3 SEP 0 7 2004 PATENT & TRADEMARK OFFICE

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **September 2, 2004**

The fee for filing this Appeal Brief is: $330.00

☐ A check in the amount of the fee is enclosed.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **09-0469 (IBM)**

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Dated: **September 2, 2004**

_____
Signature

John A. Merecki
Reg. No. 35,812
Hoffman, Warnick & D'Alessandro LLC
Three E-Comm Square
Albany, New York 12207
(518) 449-0044

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 Cf. : 1.8(a)] on

(Date) 09/02/2004

_____
Signature of Person Mailing Correspondence

Jennifer Shafer

Typed or Printed Name of Person Mailing Correspondence

CC:

P30LARGE/REV05

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Tresser

Examiner: Elisca, P.

Application No.: 09/779,954

Art Unit: 3621

Filed: 2/9/2001

Dkt. No.: CHA9-2001-0001US1

For: SYSTEM AND METHOD FOR
MAINTAINING CUSTOMER PRIVACY

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS

This is an appeal from the Final Rejection dated May 7, 2004, rejecting claims 1-

19. This Brief is accompanied by the requisite fee set forth in 37 C.F.R. 1.17 (c).

REAL PARTY IN INTEREST

International Business Machines Corporation is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

STATUS OF CLAIMS

As filed, this case included claims 1-19, which remain pending. Claims 1-19

stand rejected and form the basis of this appeal.

1

STATUS OF AMENDMENTS

Appellant filed an After-Final Response on July 7, 2004. An Advisory Action

stating that the Response was considered but did not place the application in condition for

allowance was mailed on August 9, 2004.

SUMMARY OF THE INVENTION

The invention relates to a system and method that will allow for the gathering of

business intelligence information in a network environment in a manner that will ensure

the privacy of a consumer even in a case where the consumer must reveal his or her

identity. The invention includes separating data associated with an institution into a first

database of private data and a second database of public data, storing an encrypted copy

of the private data and an unencrypted copy of the public data with an intermediary

service provider, providing to the customer a security system that allows the customer to

decrypt the encrypted data and remain anonymous to the intermediary service provider,

merging the encrypted copy of the private data and the unencrypted copy of the public

data; and providing an interface that allows the customer to view the merged data.

ISSUES

1. Whether claims 1-19 are unpatentable under 35 U.S.C. 103(a) over Clark et al., U.S.

Patent 5,710,889 ("Clark") in view of Jai et al., U.S. Patent 5,991,402 ("Jai").

GROUPING OF CLAIMS

Claims 1-19 stand or fall together.

ARGUMENT

Appellant submits that claims 1-19 are allowable and respectfully requests

reversal of the Final rejection. Claims 1-19 stand rejected under 35 U.S.C. 103(a) over

Clark et al., U.S. Patent 5,710,889 ("Clark") in view of Jai et al., U.S. Patent 5,991,402

(Jai").

To establish a *prima facie* case of obviousness, three basic criteria must be met.

First, there must be some suggestion or motivation, either in the references themselves or

in the knowledge generally available to one of ordinary skill in the art, to modify the

reference or to combine reference teachings. Second, there must be a reasonable

expectation of success. Finally, the prior art reference (or references when combined)

must teach or suggest all the claim limitations. Appellant respectfully submits that Clark

and Jai, taken alone or in combination, fail to meet each of the three basic criteria

required to establish a *prima facie* case of obviousness. As such, the rejection under 35

U.S.C. 103(a) is defective.

In the above-referenced Final Office Action, the Examiner alleges that Clark's

system includes an institutional server for delivering institutional data to a customer,

"wherein the institutional server includes a system for separately serving a first database

containing private and a second database (see., fig 1, abstract, col 3, lines 18-35,

repository and archive facility)." Independent claim 1 (and similarly independent claims

10, 14, and 18), however, includes an institutional server, wherein the institutional server

3

includes a "system for separately serving a **first database containing private data** and a **second database containing public data**." Clark fails to teach or suggest separate first and second databases containing private and public data, respectively. On the contrary, the repository and archive facilities of Clark, which the Examiner equates with the claimed first database containing public data and second database containing public data, respectively, are used to store the same type of data. Specifically, as disclosed in col. 6, lines 30-35, the repository 11 maintains a record of all messages sent through the global interface device (GID) 10. After a predetermined period of time has elapsed (e.g., 45 days), the messages are moved from the repository 11 to a secondary archive facility 18. Clearly, the same type of data (i.e., messages) is stored in both the repository 11 and the archive facility 18; Clark provides no disclosure regarding the separate storage of private and public data in different databases as claimed.

It should be noted that the Examiner's statement that Clark discloses an institutional server including a "system for separately serving a first database containing **private** and a second database" is confusing and incomplete. What is a "private"? Is the Examiner alleging that the second database contains a certain type of data? Clarification of this statement is once again requested by Appellant.

Claim 1 also includes a "service provider, wherein the service provider includes a system for **receiving an encrypted version of the private data and an unencrypted version of the public data from the institutional server**." Clark's system clearly fails to teach or suggest such a service provider. Similarly, Clark's system clearly fails to teach or suggest the claimed step of "storing an encrypted copy of the private data and an unencrypted copy of the public data with an intermediary service provider," (claim 10),

4

the claimed step of "loading to a client the encrypted private data from the institution and the unencrypted copy of the public data from the service provider," (claim 14), and the claimed "system for providing a copy of the second database of unencrypted data to an intermediary service provider" (claim 18).

In the Final Office Action, the Examiner equates Clark's on-line transaction processors (OLTPs) 12(1,2, ... n) with the claimed "service provider." In particular, the Examiner states that the "customer connects to the system whenever desired to access each of the services, and the interface device stores and routes messages between the customers and each of the **service providers** at the respective times when the customers' facilities and the **service providers'** facilities are operative." Contrary to the claimed invention, however, Clark's OLTPs do not receive private and public data that is separately served from a first database containing private data and a second database containing public data.

The Examiner alleges that Clark fails to disclose an "encrypted version of the private data and an unencrypted version of the public data." The Examiner attempts to remedy this glaring deficiency of Clark by relying on Jai. In particular, the Examiner states that Jai "discloses a method/system that enables software-on-demand and software subscription services based on a dynamic transformation filter." The Examiner also states that an "encrypted material installed on the computer is encrypted by decrypting a first version of the material to produce an unencrypted version." This statement makes no sense whatsoever. It is not clear how **encrypted** material can be **encrypted** by "**decrypting** a first version of the material to produce an **unencrypted** version." Clarification of this confusing statement is requested.

5

Appellant submits that Clark and Jai fail to teach these, as well as other numerous claim features of the present invention. For instance, with regard to claim 1, the Examiner appears to allege (see above) that Clark teaches an institutional server for separately serving a first database of private data and a second database of public data. However, no such distinction is made between private and public data in Clark. On the contrary, Clark only discloses the serving of "private" messages to customer facilities 12, wherein the messages are communicated from repository 11 to a customer facility(ies) 12 only in response to an approval by entitlement system 16. Claim 1 further recites "a service provider, wherein the service provider includes a system for receiving an encrypted version of the private data and an unencrypted version of the public data from the institutional server." As stated above, Clark fails to disclose a service provider that receives encrypted private data and unencrypted public data from an institutional server. Further, since Clark fails to disclose an institutional server for separately serving a first database of private data and a second database of public data, Clark cannot possibly disclose the display of a merged version of the private and public data. In the Office Action, the Examiner alleges that this feature is disclosed in FIGS. 15, 17, 20, 23, 24, 28, and in col. 6, lines 37-47, col. 14, lines 10-22, and col. 21, lines 16-25. However, the Examiner has made no attempt to distinguish between private and public data in any of these FIGS./sections of Clark. Clarification is again requested.

Attempting to modify Clark using Jai fails to remedy these numerous deficiencies. Jai teaches a system that resides on a computer operating system and essentially allows encrypted material to remain encrypted if it is to be delivered over a network, or be decrypted if it is required by an operating system component. Jai's system resides at a

6

single critical data path in a computer operating system. Jai does not teach or suggest a system for processing **separate** databases of encrypted material and unencrypted material. Accordingly, there is no suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify Clark or to combine Clark and Jai in the manner suggested by the Examiner, nor is there a reasonable expectation of success.
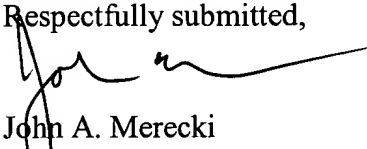
Moreover, Jai specifically teaches away from the concept of an intermediate service provider that receives "an encrypted version of the private data and an unencrypted version of the public data." Jai explicitly states that the "apparatus utilized in this invention **does not create any intermediate storage** of decrypted material that is under the protection of this technology." (See column 3, lines 24-27.) Accordingly, a person skilled in the art would clearly not be motivated to combine the two references.

Furthermore, there is clearly no teaching in either reference that allows a customer to "remain anonymous to the intermediary service provider," as recited in claims 3, 10, 14, and 18. The Examiner's position that Jai discloses this in the abstract, Figure 1 and item 108 is clearly without merit, as Jai teaches away from an intermediary service provider; the abstract makes no mention of anonymity; and Figure 1 and item 108 do not show any mechanism for allowing a customer to remain anonymous. Appellant appreciates the Examiner's voluminous recitation of case law regarding obviousness. However, the Examiner has not directly addressed any of the arguments presented by Appellant to date, and repeated above, regarding the lack of establishment of a *prima facie* case of obviousness.

In summary, Appellant submits that claims 1-19 are allowable because Clark and Jai, taken alone or in combination, fail to meet each of the three basic criteria required to establish a *prima facie* case of obviousness.

Respectfully submitted,

John A. Merecki
Reg. No. 35,812

Date: 9/2/04

Hoffman, Warnick & D'Alessandro LLC
Three E-Comm Square
Albany, New York 12207
(518) 449-0044
(518) 449-0047 (fax)

APPENDIX

1. A system for delivering institutional data to a customer, comprising:

an institutional server, wherein the institutional server includes a system for separately serving a first database containing private data and a second database containing public data;

a service provider, wherein the service provider includes a system for receiving an encrypted version of the private data and an unencrypted version of the public data from the institutional server; and

a client, wherein the client includes a system for displaying a merged version of the private and public data.

2. The system of claim 1, wherein the client includes a mechanism for decrypting the encrypted private data.

3. The system of claim 1, further comprising a system for making the customer anonymous to the service provider.

4. The system of claim 3, wherein the system for making the customer anonymous to the service provider includes a mechanism for determining a service level available to the customer.

5. The system of claim 1, wherein the service provider includes a system for analyzing the use of the public data by the customer without knowing an identity of the customer.

6. The system of claim 1, wherein the merged version of the private and public data is downloaded to the client by the service provider.

7. The system of claim 1, wherein the private and public data are downloaded to the client by the institutional server and service provider, respectively.

8. The system of claim 1, wherein the encrypted version of the private data is encrypted using a public key infrastructure protocol.

9. The system of claim 1, wherein the client includes an interface that can be customized into a first window for viewing the public data and a second window for viewing the private data.

10. A method of preserving privacy between a customer and an institution in a computer network environment, comprising the steps of:

    separating data associated with the institution into a first database of private data and a second database of public data;

    storing an encrypted copy of the private data and an unencrypted copy of the public data with an intermediary service provider;

providing to the customer a security system that allows the customer to decrypt the encrypted data and remain anonymous to the intermediary service provider;

merging the encrypted copy of the private data and the unencrypted copy of the public data; and

providing an interface that allows the customer to view the merged data.

11. The method of claim 10, wherein the security system includes a public key infrastructure protocol.

12. The method of claim 10, comprising the further step of customizing the interface to include a first window for viewing the public data and a second window for viewing the private data.

13. The method of claim 10, wherein the public data includes data available externally to the institution.

14. A method of preserving privacy between a customer and an institution in a computer network environment, comprising the steps of:

separating data associated with the institution into a first database of encrypted private data and a second database of public data;

loading an unencrypted copy of the public data to a service provider;

loading to a client the encrypted private data from the institution and the unencrypted copy of the public data from the service provider;

providing to the customer a security mechanism that allows the customer to decrypt the encrypted data and remain anonymous to the service provider; and

providing an interface that allows the customer to view the encrypted copy of the private data and the unencrypted copy of the public data.

15. The method of claim 14, wherein the security mechanism includes a public key infrastructure protocol.

16. The method of claim 14, comprising the further step of customizing the interface to include a first window for viewing the public data and a second window for viewing the private data.

17. The method of claim 14, wherein the public data includes data available externally to the institution.

18. A program product stored on a recordable medium that when executed, preserves privacy between a customer and an institution in a computer network environment, comprising:

a system for separating data associated with the institution into a first database of encrypted data and a second database of unencrypted data;

a system for providing a copy of the second database of unencrypted data to an intermediary service provider;

12

an interface that allows the customer to view the first database of encrypted data

and the copy of the second database of unencrypted data provided to the intermediary

service provider; and

a security system that allows the customer to decrypt the encrypted data and

remain anonymous to the intermediary service provider.

19. The program product of claim 18, further comprising:

a system for providing a copy of the first database of unencrypted data to the

intermediary service provider.